UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/717,647	11/21/2003	Song-Yean Cho	Q78056	9133

23373   7590   10/30/2007
SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER
DALEY, CLIFTON G

ART UNIT	PAPER NUMBER
2624	

MAIL DATE	DELIVERY MODE
10/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>21 November 2003</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-7</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-7</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>19 March 2004</u> is/are: a)☐ accepted or b)☒ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

       1.☒ Certified copies of the priority documents have been received.

       2.☐ Certified copies of the priority documents have been received in Application No. _____.

       3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date <u>2/23/2004, 3/29/2007</u>.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____ .

DETAILED ACTION

Drawings

1.   Figures 1 and 2 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

2.   The drawings are objected to because in Figure 2, the block labeled "Multimedia data producer (A)" is implied in the specification to be Multimedia data receiver (A). The examiner interprets the label to be "Multimedia receiver (A)". Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief

description of the several views of the drawings for consistency. Additional replacement

sheets may be necessary to show the renumbering of the remaining figures. Each

drawing sheet submitted after the filing date of an application must be labeled in the

top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d).

If the changes are not accepted by the examiner, the applicant will be notified and

informed of any required corrective action in the next Office action. The objection to the

drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4.   Claims 1, 2, 6 and 7 are rejected under 35 U.S.C. 102(b) as being anticipated by

Tang (Lei Tang, "Methods for encrypting and decrypting MPEG video data efficiently",

1997, Proceedings of the fourth ACM international conference on Multimedia, pp. 219-

229)

Regarding claims 1 and 6, Tang teaches a method and analogous apparatus

for encrypting and compressing multimedia data, comprising the steps of: creating

Discrete Cosine Transform (DCT) coefficients by applying input multimedia data to a

DCT unit, and quantizing the created DCT coefficients **(Figure 1, § 2, ¶ 1, and § 3, ¶**

2); encrypting and compressing a transformed Differential Coefficient (DC coefficient)

and a transformed Amplitude Coefficient (AC coefficient) by transforming encoded DC

and AC coefficients depending on a certain encryption key at the time of entropy

encoding quantized DC and AC coefficients of the quantized DCT coefficients **(page**

223 § 4.3, ¶ 1, lines 1-3, i.e. the 8x8 block consists of the DC coefficient and

all AC coefficients. The 1x64 list is the encryption key (page 223, § 4.2, ¶ 2,

lines 5-6), and "Zig-zag" pattern in Figure 1 replaced with encrypted order

(page 223, § 4.2, ¶ 2)); and Huffmann coding the encrypted DC and AC coefficients

using a Huffmann table and outputting the coded DC and AC coefficients **(page 226, §**

5, ¶ 5 (last paragraph), lines 9-12).

        Regarding claims 2 and 7, Tang teaches the method and analogous

apparatus according to claim 1, wherein the step of encrypting and compressing the DC

and AC coefficients comprises the steps of: performing Differential Pulse Code

Modulation (DPCM) of the quantized DC coefficient and Run Length Coding (RLC) of the

quantized AC coefficient **(page 221, Figure 1 and page 221, right column, item 4,**

Zig-zag scan); determining the encryption key of the AC and DC coefficients and a

random constant r indicating a start bit of the encryption key, using variable length

information including a Variable Length Code (VLC) and a Variable Length Integer (VLI),

of each of the DC and AC coefficients obtained through the DPCM and the RLC **(page**

225, § 4.5, ¶ 4 (last paragraph), lines 10-16, i.e. random constant r

determines permutation list); and encrypting the AC and DC coefficients using the

determined encryption key **(i.e. by changing the zig-zag order via the**

permutation list disclosed above).

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6.   Claims 3-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tang

as applied to claim 2 above, and further in view of Shi et al. (Hereinafter "Shi":

Changgui Shi and Bharat Bhargava, "An Efficient MPEG Video Encryption Algorithm",

1998, IEEE, pp381-386).

Regarding claim 3, Tang teaches the method according to claim 2, wherein

the step of encrypting the AC and DC coefficients comprises the step of: determining

whether a value of an r-th bit is "1" in the determined encryption key of the DC

coefficient **(page 225, § 4.5, ¶ 3, i.e. the encryption key "k" is determined,**

therefore whether a value of an r-th bit is "1" is inherently determined).

Tang does not teach the step of transforming the DC coefficient by performing

an exclusive logical sum operation between the VLC of the DC coefficient and 11111111

if the determined value is "1".

However, Shi discloses an encryption step of transforming the DC coefficient by performing an exclusive logical sum operation between the VLC of the DC coefficient and 11111111 if the determined value is "1" **(page 383, § 4, ¶ 3, i.e. Shi discloses transforming the VLC of the DC coefficient based on whether a value of an r-th bit in the determined encryption key is "1")**.

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have added Shi's encryption step to Tang's encryption method, in order to improve encryption while adding minimal overhead **(Shi: Abstract)**.

Regarding claim 4, Tang teaches the method according to claim 2, wherein the step of encrypting the AC and DC coefficients comprises the step of: determining whether a value of an r-th bit is "1" in the determined encryption key of the AC coefficient **(page 225, § 4.5, ¶ 3, i.e. the encryption key "k" is determined, therefore whether a value of an r-th bit is "1" is inherently determined)**.

Tang does not teach the steps of right-shifting the VLI of the AC coefficient if the determined value is "1"; determining the VLC of the AC coefficient through the right-shifted VLI using the Huffmann table; and transforming the AC coefficient using the determined VLC and VLI.

However, Shi discloses the steps of right-shifting the VLI of the AC coefficient if the determined value is "1" **(page 383, § 4, ¶ 3, i.e. Shi discloses transforming the VLI of the AC coefficient based on whether a value of an r-th bit in the determined encryption key is "1")**; determining the VLC of the AC coefficient

through the right-shifted VLI using the Huffmann table **(Tang: Figure 1, i.e.**

standard MPEG compression procedure); and transforming the AC coefficient

using the determined VLC and VLI **(i.e. result of previous two steps)**.

Therefore it would have been obvious to one of ordinary skill in the art at the

time of the invention to have added Shi's encryption steps to Tang's encryption method,

in order to improve encryption while adding minimal overhead **(Shi: Abstract)**.

Regarding claim 5, Tang in combination with Shi teaches the method

according to claim 4, wherein the encryption key includes first and second symmetric,

and the symmetric keys are VLCs of the AC and DC coefficients, respectively keys

(Tang: page 225, § 4.5, ¶ 3, i.e. using DES, the NIST encryption standard, for

the DC coefficients, and Shi recommends encryption for both DC and AC

coefficients, Shi: page 385, left column, lines 1-3).

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Clifton G. Daley whose telephone number is 571-270-

3144. The examiner can normally be reached on Monday - Friday 7:30am - 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Samir Ahmed can be reached on 571-272-7413. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO

Customer Service Representative or access to the automated information system, call

800-786-9199 (IN USA OR CANADA) or 571-272-1000.

                                        Samir Ahmed
                                        SPE
                                        Art Unit 2624

CGD
10/17/2007
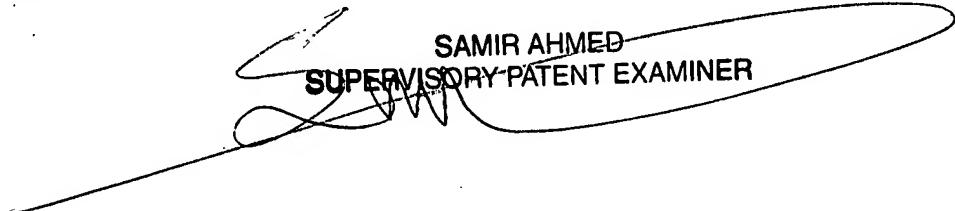
SAMIR AHMED
SUPERVISORY PATENT EXAMINER